ISSN:0975-9646

Effective Authentication Mechanisms for Mobile Devices :Smartcard(SMCA,BSCA)

1. Amjan Shaik , *CSE, Ellenki College Of Engineering and Technology(ECET), Patelguda,Hyderabad.*
2. Dr.C.R.K.Reddy, *CSE, Chaitanya Bharathi Institute Of Technology (CBIT), Gandipet, Hyderabad.*
3. Mohd Mukarram Uddin , *CSE,Moghal College Of Engineering andTechnology(MCET),Bandlaguda,Hyderabad.*

ABSTRACT:
This is an era of mobile communications and computing where mobiles are being used in place of traditional computers. Mobile devices are small, handy devices that can be carried around by the user very easily. A user holding the mobile device will have access to the information even at the places where no internet terminal is available. Due to this reason, they are heavily being used in the business environment in managing application, e-mail correspondence, accessing the remote corporate data, handling voice calls, etc. But the mobile devices are still lack-in most important security features such as user authentication, content encryption, virus protection, confidentiality, integrity, etc. The sensitive information stored in the mobile devices is not secure (can be accessed by an unauthorized user). Mobile device poses limited storage and processing power, and the low battery-power. It is also tedious to implement the cryptographic algorithms on mobile devices because they need heavy computations such as generating a key as a large prime numbers. Hence, many security threats are possible when mobile device is used. One of the most serious security threats is the unauthorized use of the mobile device. It is very common that mobile devices can be used by unauthorized person because they are handy and can be lost or stolen very easily. A smart card used with mobile device resist its 'unauthorized use'. The limited computation capabilities of the mobile can also be enhanced by using the smart cards. In this paper , two novel types of smart cards such as Smart Multimedia Card Authentication(SMCA) and Bluetooth Smart Card Authentication (BSCA) are used. The authentication mechanisms proposed in this paper are based on Multimode Authentication Framework, which provides a flexibility to add our own authentication modules. The developed authentication mechanisms provide the dual-security to the mobile devices and are well enough to resist the attacks which are possible over mobile devices. Demand for competent software is rising day by day and object-oriented design procedure became able to fulfill this demand because it is the most powerful mechanism to develop efficient software systems. It can not only help in reducing the cost but also helps in the development of high quality software systems. Software developers need appropriate metrics to develop efficient software system. Object-oriented metrics can play vital role[10,11] in this aspect due to their importance in the development of successful software applications. Empirically we analyzed and deliberate the OO Metrics also in this paper.

Keywords: Smart Card , SMCA. BSCA, Metrics, DIT, NOC, Measurement.

1.INTRODUCTION:

Today's mobile devices are multi-functional devices capable of hosting a broad range of applications for both business and consumer use. The mobile devices such as PDA's(Personal Digital Assistants) and the ever-growing category of smart phones allow people to access the Internet for e-mail, instant messaging, text messaging and Web browsing and many more. The mobile devices are often seen as an extension to your own PC. Work done on the road or away from the office can be synchronized with your PC to reflect changes and new information. As per the survey made by the year 2010, it is observed that more than 800 million people around the world accessed the internet. Due this fact, the mobile devices with internet services such as WAP (Wireless Application Protocol) and i-Mode (packet-based service for mobile phones) are being used rather than personal computer[1,3].

Mobile devices have wireless capability to connect to the Internet and office/home computer systems. However wireless capability poses a number of security risks such as attacks on confidentiality, authentication, and integrity. Therefore, the mobile devices should be designed to be resistant against these security risks. In this paper various attacks are analyzed and an authentication mechanism is developed as a solution to strengthen the security of mobile device. We have considered the latest technology used for mobile devices and smartcard. Both the technologies are growing at their own speed to fill the processing capability gap with PCs. The combination of mobile device and a smartcard poses enough computation power to implement the authentication process and a better cryptographic algorithm can be used. Hence, RSA algorithm is used to generate the electronic signatures for the mobile device and smartcard. A developed authentication mechanism provides a dual security to the mobile user i.e. a user should hold both the smartcard and security token to initiate an authentication process through the mobile device. The proposed authentication mechanisms are known as Smart Multimedia Card Authentication (SMCA) and Bluetooth Smartcard Authentication (BSCA). Both SMCA and BSCA are based on Multimode Authentication Framework (MAF). The DIT (Depth of Inheritance Tree) will be the maximum length from the node to the root of the tree. The deeper a class is in the hierarchy, the greater the number of methods it is likely to inherit, making it more complex to predict its behavior. The NOC (Number of Children) is the number of immediate subclasses subordinated to a class in the class hierarchy. It is a measure of how many subclasses are going to inherit the methods of the parent class. The number of children gives an idea of the potential influence a class has on the design. If a class

has a large number of children, it may require more testing of the methods in that class. The Greater the number of children (NOC), greater the likelihood of improper abstraction of the parent class. If a class has a large number of children; it may be a case of misuse of sub classing[10,11].A multi-mode authentication is taken as a platform which implements the organizational policies at various security levels. It provides multiple levels of authentication for a single user as per the privileges hold by him. Hence, the user even after the authentication is restricted to the privileges assigned by the organization. As a result, it increases the effort required to compromise the device mainly from unauthorized use.

2. SMARTCARD :

A smartcard is a plastic card that hold embedded computer chip (microprocessor chip) which contains operating system, program and data. In laymen terms – "Smartcard is a very small computer embedded on a plastic card". Smartcards can be embedded with either a microprocessor and memory chip or only a memory chip. Microprocessor chips inbuilt with non-programmable logic which allows user to add, delete, or manipulate the information stored on the card while a memory-chip card allows only a pre-defined operation such as decrements the talk time stored in pre-paid phone cards. Sometimes smartcards can also be termed as Integrated Circuit Card (ICC) and defined as a portable, tamper-resistant computer containing a programmable data store. The IC embedded in the card has features through which data can be transferred, stored and processed[8,9].

Smartcards and magnetic-stripe cards are the two most popular types of cards and can be found in every wallet. Smartcards contain all necessary functions and information on the card. Unlike magnetic stripe cards, they do not require access to remote databases at the time of the transaction. One of the most important qualities of a smartcard is the possibility to protect data stored on the card against unauthorized access and manipulation. A smartcard's operating system controls the interface for transferring data between the smartcard and a connected card reader. The data stored into the smartcard can be prevented from being read by unauthorized user with the help of cryptographic algorithms and security protocols.

2.1 Construction

The main storage area in the smartcards is normally EEPROM, which have contents in it and retains them even when the power is off. Smartcard chips may also have math co-processors integrated into the microprocessor chip, which is able to perform complex encryption routines quite fast. The construction of the smartcard is shown in Figure 1. The chip connections can be either a contact or contact less. They are connected to the card reader either via a direct physical contact or remotely via a contact less electromagnetic interface. A smartcard is uniquely characterized by its embedded chip which maintains data within an extremely secure environment[5]. The secret keys of the cryptographic systems can be kept safe in smartcard so that it is protected against the most sophisticated forms of attack. In turn, the used cryptographic system protects the integrity and privacy of card-related communications.

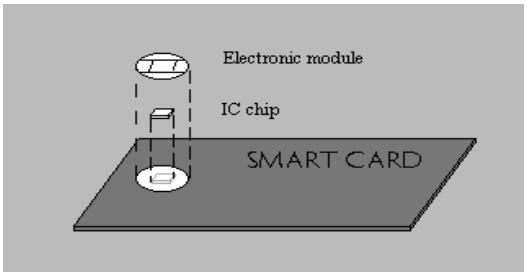

Figure 1: Smartcard's Construction

2.2 Card Operation:

The smartcards need electrical power from a external source, plus it requires a device which can read the data from it, transmit the response back to the chip. The smartcards interact with an "accepting device", usually known as a card reader, which exchanges data with the card and usually involves the electronic transfer of money or personal information. The information or application stored in the IC chip is transferred through an electronic module that interconnects with a terminal or a card reader.

Smartcard Attributes	Maximum Data Capacity	Processing Power	Cost of Card	Cost of Reader and Connection
Magnetic Stripe Cards	140 bytes	None	$0.20 - $0.75	$750
Memory Cards	1 Kbytes	None	$1 - $2.50	$500
Processor Cards	8 Kbytes	8-bit CPU, moving to 16- and 32-bit	$7-$15	$500
Optical Memory Cards	4.9 Mbytes	None	$7 - $12	$3,500 - $4,000

Table 1: The comparison among various types of smartcards

This year, almost 1 billion smartcards will be produced worldwide by several big manufacturers. Currently, 95% of these cards are issued in Europe, South America, and Asia. By the year 2000, Data Monitor predicts that over 3 billion cards will be in circulation worldwide - with over 15% of the total in use in the

United States and Canada. With the help of this comparison, it is observed that there are over 1000 million credit cards in circulation today. Major uses will include providing enhanced financial services, increasing the security and flexibility of *cellular phones*, and securing satellite and cable transmissions in TV set-top boxes.

COS Name	Producer
GemXplore, MPCOS, GPK	Gemplus
STARCOM, STARSIM. STARDC	Giesecke and Devrient
Multos	Maosco
AuthenticIC, SIMphonic	Oberthur
Micardo	Orga
Cyberflex, Multiflex, Payflex	Schlumberger
CardOS	Siemens
TCOS	Telesec

Table 2: Smartcard operating systems and their producer

Smartcards poses low processing capabilities, it will be painful to optimize the cryptographic functions so that operating system executes them in a very short duration. The smartcard's operating system doesn't support multi-tasking capabilities just to provide the required level of reliability for its components. COS should perform the following primary tasks:

- Transfer the data to and from the smartcard
- Control the execution of the commands
- Manage the files and data held in memory
- Manage the card security and cryptographic algorithm procedures and also maintains the reliability, particularly in terms of data integrity.
- Access control to information and functions (e.g. controls the permissions given for a particular file for read, write, or execute)

Earlier, smartcards were costly and inflexible, but now the trend is towards multi-application cards. For on-card application development of programs that run inside the secure environment of the smartcard chip, two operating systems i.e. Java Card and MULTOS are recommended. These two are flexible, reliable and have good exposure in today's market[4,9].

3 SMARTCARD AUTHENTICATION MECHANISMS:

Two effective authentication mechanisms which are compact and fully compatible with the capabilities possessed by mobile devices. These authentication mechanisms can be developed by using two novel types of smartcards i.e. Smart Multimedia Card (SMC) and Bluetooth Smartcard (BSC). SMC is the contact based smartcard whereas BSC is a contact less smartcard. Both cards are compact in size and best suitable for the mobile devices unlike standard sized smartcards. The authentication mechanism developed by using SMC is termed as SMC Authentication (SMCA). In the same way, authentication mechanism developed by BSC is termed as BSC Authentication (BSCA). They can be implemented on MAF which provides a facility to add new authorization mechanism modules. MAF consist of two parts as Authentication handler and User interface. Authentication handler is embedded with procedure that performs authentication process. User interface performs all necessary interactions with user.

3.1 Smart Multimedia Card Authentication (SMCA) Mechanism

SMCA depends on smartcard chip packaged in multimode card format. This card is stamp sized card houses a multimedia controller, smartcard, and a flash memory. Every smartcard poses unique smartcard security token. The security token can be a PIN possessed by a particular user. This token has been utilized during authentication process. Handler software runs in the user space on handheld device. Handler monitors the card insertion and removal. It also controls the necessary steps authentication process. SMC handler operates in two modes. In one mode, it acts as a polling handler which periodically checks the status of smartcard. In other mode, it acts as an authenticator which performs actual authentication with smartcard. Authentication is accomplished by obtaining PIN from user and APDU's are used to create authentication session. Device issues the challenge and verify the response from smartcard Figure2. shows the initial exchange used to enroll a smartcard token at right with handheld device at left. Lower part shows the exchanges used to verify the claimed identity. The Challenge-Response protocol is used to verify the authorized user.

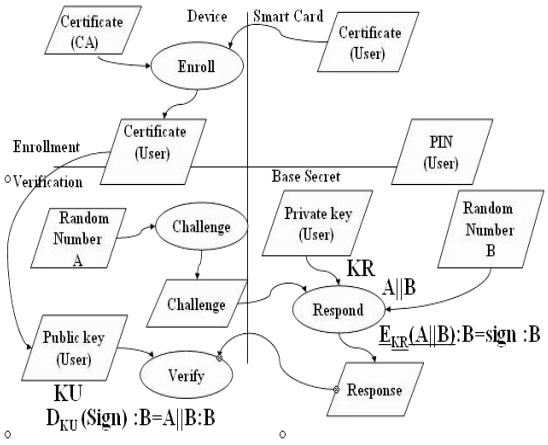

Figure 2: Challenge-Response Exchange

The procedure which is needed to follow should be in following sequence:

- The device acts as verifier, generates a random challenge "A" and passes it to the smartcard to be

signed with private key associated with the enrolled identity certificate.

- The smartcard acts as the claimant, generates a random number "B" and signs A||B with private key on the card (|| denotes concatenation).As a response to the retrieved challenge it returns "B" and signature to the device.
- The devices retrieves the response, verifies the card's signature over A||B using the public key in the certificate.
- If everything successfully verifies, authentication succeeds, otherwise authentication fails.

Enroller applet supports a set of APDUs that provide functionality of RSA for encryption/decryption process and X.509 Certification process.

3.2 Bluetooth Smartcard Authentication (BSCA) Mechanism

As similar to SMCA, BSCA also depends on smartcard chip. It uses wireless interface and doesn't require any physical contact to connect smartcard to handheld devices. This mechanism provides high security having merits:

- It doesn't require smartcard reader
- Smartcard is well compact in size
- It works even at a distance of few meters
- It is not necessary that device should be in direct line of sight of smartcard
- It can be a discrete (i.e. communication between them is not discovered by the third party).

A BSC token houses a Bluetooth radio, smartcard, processor, memory and battery. In addition it can be equipped with display and keypad to accept PIN. In many aspects Bluetooth smartcard has similarities with SMC i.e. it depends on functionality of a Java Card applet, uses the challenge-response protocol for card authentication, and implemented on MAF environment. It differ from SMC from communication point of view, the communication between device and token takes place using a Bluetooth channel rather than an MMC bus. Another difference is that PIN entry is allowed at the BSC token side rather than at the handheld device.

4. SEQUENTIAL DIAGRAM SURVEY:

UML sequence diagrams model the flow of logic within your system in a visual manner, enabling you both to document and validate your logic, and are commonly used for both analysis and design purposes. Here the sequential flow of the entire process is given starting with the device and smartcard enrollment of the device is being carried out then verification process is being carried out, if it is success then user can able to access the service otherwise can't able to access the services.

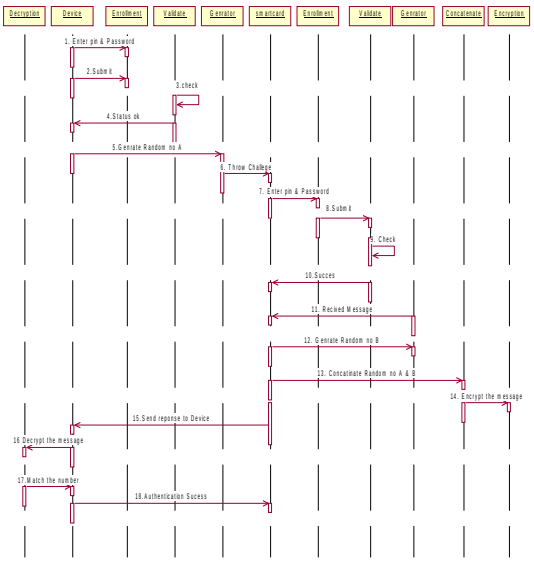

Figure 3: Sequential Diagram for Device and Smartcard

5. CLASS DIAGRAM SURVEY:

A Class diagram is a type of static structure diagram that describes the structure of a system by showing the system's classes, their attributes, and the relationships between the classes. Here the sequential flow of the entire process is given starting with the device and smartcard enrollment of the device is being carried out then verification process is being carried out, if it is success then user able to access the service otherwise the not able to access the services.

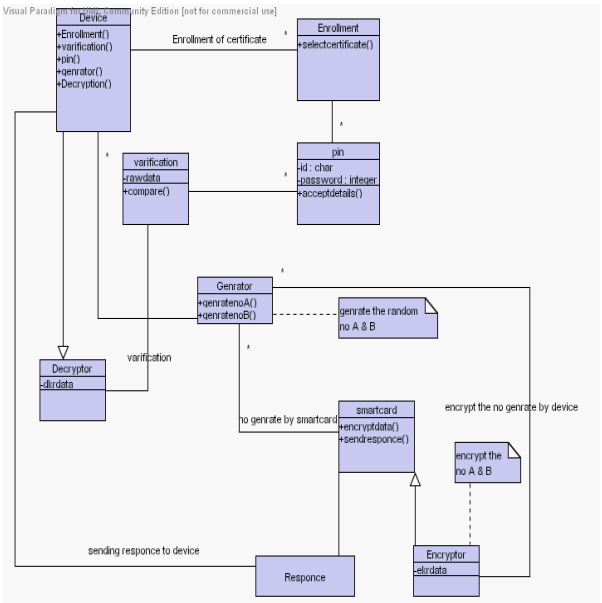

Figure 4: Class Diagram for Device and Smartcard

6.Validations:

Test Case ID	Description	Input	Output
1	user selects a correct certificate which is displayed on device	Sun certificate 1	Success
2	user selects a correct certificate which is displayed on device	Sun certificate 2	Success
3	user selects a correct certificate which is displayed on device	Microsoft's certificate	Failure
4	user selects a correct certificate which is displayed on device	None	Failure

Table 3: Device prompts the user to enroll the certificate

Test Case ID	Description	Input	Output
1	After enrollment device gives two choices to the user as *Continue*/*Exit*	Selects *Continue*	PIN verification carried out
2	*Username* and *Password* are the text fields which prompt the user to enter his name and the PIN number associated with the smartcard.	Enter Username and Password Ex:User: smart, Pass: card	Success
3	Invalid username and password is given is redirected to restart the application to reenter the personal details.	ABCD 12345	Failure
4	Device generates the random number	Seed value	Success
5	Smartcard generates a another random number	Seed value	Success

Table 4: Device prompts the user to perform Authentication process with the help of Smartcard

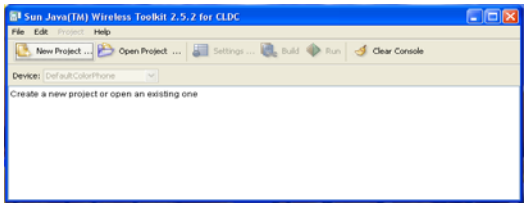

Figure 5: The main window of the wireless toolkit

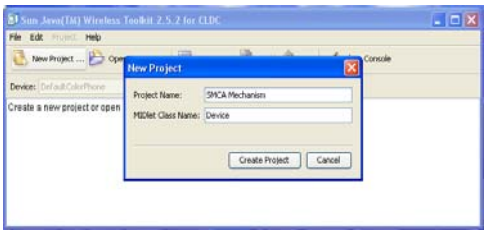

Figure 6: A dialog which creates the project

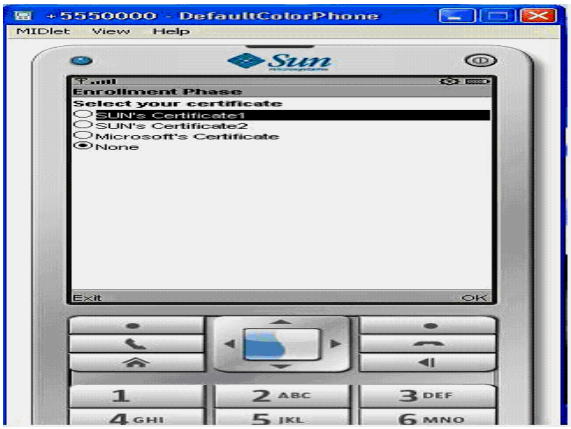

Figure 7: Device prompts the user to enroll the certificate

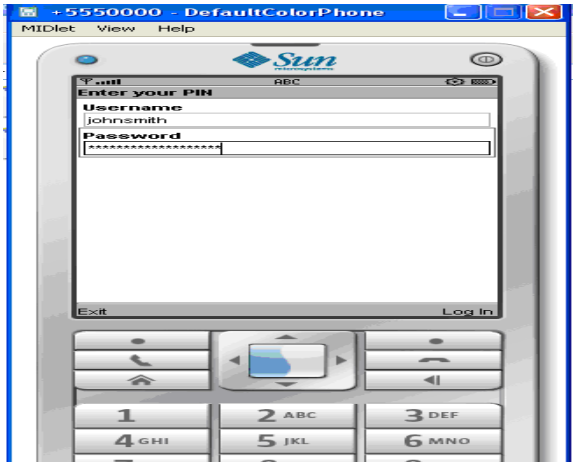

Figure 8: Device prompts the user to enter username and password

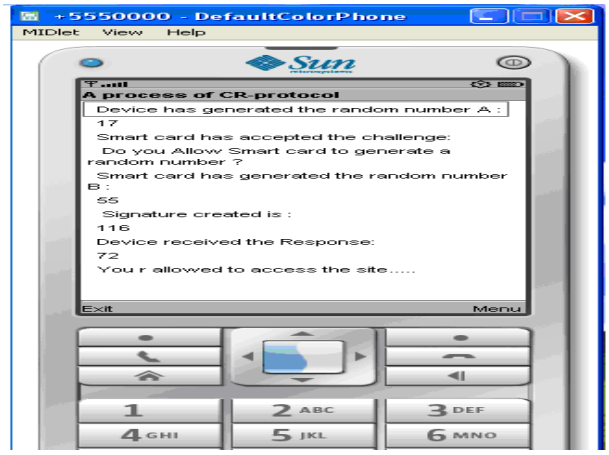

Figure 9: Mobile device shows the complete C-R protocol process

7.CONCLUSION:

Mobile devices such as PDA's, smart phones, or any other handheld device are very useful for accessing remote repositories but poses certain security risks. They are lack in providing important security features such as user authentication, content encryption and virus protection etc. As the smartcards are known for its tamper-resistant quality, the SMCA is developed by using the smartcards which are compatible with mobile devices. The proposed SMCA is termed as the best solution against the unauthorized use of the mobile devices because it allows only the authorized users to use a mobile device. The SMCA also support MAF to provide multiple modes of authentication. As a result, it increases the effort to compromise a device and allow users to select different levels of security to make the information as secure as possible. The document is aimed to add the *user authentication* and *organizational policies* as a security features into mobile devices. With the help of this two features a mobile device can be used effectively only by the authorized user without any fear of losing to stored secret information. An organizational policy ensures the organization that the same privileges are provided for the users who access its resource from the PC, PDA, or any other handheld device. In this paper we presents two mechanisms for user authentication. It is concluded that the variation of complexity depends on the measure of DIT (Depth of Inheritance) and NOC (Number of Children) in the context of authentication, while build SMCA,BSCA, the measure of Depth of Inheritance (DIT) with respect to Number of children (NOC) place a central role, which is evidence from the fact that the complexity depends on the depth of inheritance (DIT) with respect to Number of children (NOC). Both DIT and NOC directly relate to the design of the class hierarchy. In an SMCA,BSCA, Classes with high DIT values are associated with a higher number of defects.

ACKNOWLEDGEMENTS:

The authors thankful and appreciate the M.Tech (CSE) students and Colleagues, in Aurora's Scientific Technological and Research Academy (ASTRA) in the preparation of this work as a part of their M.Tech Project.

REFERENCES:

[1].A. J. Menezes, P. C. Oorschot, and S. A. Vanstone. Handbook of Applied Cryptography. CRC Press, Boca Raton,2007.

[2].D. R. Stinson. Cryptography: Theory and Practice. CRC Press, Boca Raton,2008.

[3].W. Diffie and M.Hellman. New Directions in Cryptography. *IEEE Trans on Information Theory*,644-654, 1976.

[4].RL.Rivest, A. Shamir, and L. M. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120 -126, 1978.,

[5].SIAM News, Volume 36, Number 5, June 2003, "Still Guarding Secrets after Years of Attacks, RSA Earns Accolades for its Founders", by Sara Robinson..

[6].Charlie Kaufman, Radia Perlman, Mike Speciner, Network Security- PRIVATE Communication in a PUBLIIC World, Second Edition.2005.

[7].http://java.sun.com/javacard/reference/docs/smartcards.html, the information is accessed on 29th May, 2008.

[8].SmartCard Handbook, By Wolfgang Rankl, Wolfgang Effing, Ebooks Corporation,2006.

[9].A Unified Framework for Mobile Device Security, The 2004 International Conference on Security and Management, June 2004. Wayne Jansen, Vlad K, Serban Gavrila, Thomas Heute, Clément Séveillac.

[10].Amjan Shaik, Dr.C.R.K.Reddy, M.Bala, "An Empirical Validation of Object Oriented Design Metrics in Object Oriented Systems International Journal of Emerging Trends in Engineering and Applied Sciences(JETEAS)Volume.1, No.2, Page 211-219, ISSN: 2141–7016, December, 2010.

[11].Amjan Shaik, Dr.C.R.K.Reddy, M.Bala ,"Metrics for Object Oriented Design Software Systems: Survey"International Journal of Emerging Trends in Engineering and Applied Sciences(JETEAS),Volume.1, No.2,Page 189-197,ISSN: 2141–7016, December, 2010.

ABOUT THE AUTHORS:

Amjan Shaik is working as a Professor and Head, Department of Computer Science and Engineering at Ellenki College of Engineering and Technology (ECET), Hyderabad, India. He has received M.Tech. (Computer Science and Technology) from Andhra University. Presently, he is a Research Scholar in JNTUH. He has been published and presented more than 30 Research Papers and Technical Papers in International, National Journals and International, National Conferences. His main research interests are Software Engineering, Software Metrics and OOAD.

Dr.C.R.K. Reddy is working as a Professor and Head, Department of Computer Science and Engineering at Chaitanya Bharathi Institute of Technology (CBIT),Hyderabad, India. He has received M.Tech.(Computer Science and Engineering) from JNTUH, Hyderabad and Ph.D in Computer Science and Engineering from Hyderabad Central University (HCU). He has been published and presented a wide range of Research Papers and Technical Papers in International, National Journals and International, National Conferences. At Present 8 Research Scholars are doing Ph.D under his esteemed guidance. His main research Interests are Program Testing , Software Engineering , Software Metrics and Software Architectures.

Mohd Mukarram Uddin is working as an Asst Professor and Head, Department of Computer Science and Engineering at Moghal College of Engineering and Technology (MCET), Hyderabad, India. He has received M.Tech (Information Technology) from ASTRA, Affiliated to JNTUH Hyderabad. He has presented number of technical papers in International and National Conferences. His research interests are Mobile Computing, Information Security and Software Engineering.